UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,081	06/20/2003	Chris L. Stone	093196-1026	6842

30542 7590 09/02/2009

FOLEY & LARDNER LLP
P.O. BOX 80278
SAN DIEGO, CA 92138-0278

EXAMINER	
DUFFIELD, JEREMY S	
ART UNIT	PAPER NUMBER
2427	
MAIL DATE	DELIVERY MODE
09/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/600,081	STONE ET AL.	
	Examiner	Art Unit	
	JEREMY DUFFIELD	2427	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4,6,7,10-33,35,36,38-40 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4,6,7,10-33,35,36,38-40 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 18 May 2009 have been fully considered but they are not persuasive.

In response to applicant's arguments, Page 11, lines 4-6, the Examiner respectfully disagrees. Alattar teaches a watermark can include additional information in the form of various identifiers which are compared to identifiers located in a database, (Col. 10, lines 10-36), and using a watermark in conjunction with a fingerprint in which the fingerprint is matched to a corresponding fingerprint in a database (Col. 20, lines 20-57). Alattar further teaches a watermark may contain an identifier for broadcast monitoring, version information, hidden auxiliary identifiers that identify content and its source, and identify which movie was broadcast, who broadcast it, and when it was broadcast (Col. 8, lines 13-36, Col. 8, line 60-Col. 9, line 4). Brunk teaches a watermark for use in conjunction with a content signature, i.e. fingerprint (Col. 6, lines 40-52; Col. 6, line 65-Col. 7, line 50). The content signature can be used to determine a content ID, licensing or registration data, other metadata, etc (Brunk-Col. 1, lines 50-64). The watermark can be used to determine owner ID, metadata, security information, copy control data, etc (Brunk-Col. 6, line 65-Col. 7, line 3). A person of ordinary skill in the art would have known the similarities in the content signature data and the watermark data and realized that the two may carry the same or very similar data, e.g. licensing/registration data-security and copy control data, other metadata-metadata, content ID-content identifying information etc, to identify the content. Therefore, the

content signature and watermark data may be used to "redundantly" identify the content.

In response to applicant's arguments that the given references do not teach "that the information...with the watermark", Page 11, lines 25-27 and 18-22, the examiner respectfully disagrees. Brunk clearly states a "content signature also can be compared to digital watermark data, and if the content signature and digital watermark data match (or otherwise coincide) the content is determined to be authentic." A person of ordinary skill in the art possessing ordinary creativity, common sense, and logic would have known that since the signature and watermark may have the same data, (see above arguments), that when compared and matched, the same data from both the signature and the watermark would be used.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 4, 6, 7, 10-14, 17-19, 24-27, 32, 33, 36, 38, 40, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alattar (US 7,020,304) in view of Brunk (US 7,289,643).

Regarding claim 2, Alattar teaches a method of tracking a broadcast program, comprising:

inserting a unique watermark value into a program to be broadcast (Col. 5, lines 59-63);

deriving a fingerprint value based on said program's content (Col. 20, lines 15-17);

storing said program's watermark value and associated fingerprint value (Col. 10, lines 10-18; Col. 20, lines 50-54);

detecting any watermark value inserted in a given broadcast program (Col. 1, lines 29-39; Col. 3, lines 10-17; Col. 8, lines 24-28; Col. 20, lines 46-51);

deriving a fingerprint value based on said given broadcast program's content (Col. 20, lines 15-17); and

creating a database in which said unique watermark(s) and their associated derived fingerprint values for a plurality of unique programs to be broadcast are stored (Col. 10, lines 10-36; Col. 20, lines 38-54);

registering said unique watermark and associated derived fingerprint value for said program to be broadcast in said database (Col. 10, lines 10-36; Col. 20, lines 38-54; Col. 4, lines 1-19 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar); and

identifying said given broadcast program, i.e. the watermark may contain broadcast monitoring, creator, distributor, and recipient information as well as

identifying which movie was broadcast, who broadcast it, and when it was broadcast (Col. 8, lines 13-36, Col. 8, line 61-Col. 9, line 4), said identification comprising:

comparing any detected watermark value with said database of registered watermark values, Note: a watermark value, according to Alattar, not only serves as a calibration signal but also can include identifiers, that relate the identifiers from the watermark to corresponding identifiers in a database that has additional information to identify the content owner, distributor, etc (Col. 10, lines 10-18);

if a detected watermark value matches a registered watermark value from said database of registered watermark values, cross-checking said fingerprint value derived from said given broadcast program against said database of registered fingerprints (Col. 20, lines 38-57).

Alattar does not clearly teach redundantly identifying said broadcast program, said redundant identification comprising: if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint to assess a status of said broadcast program.

Brunk, explicitly incorporated by reference in Alattar (Col 20, Lines 26-35) teaches creating a database in which said unique watermark(s) and their

associated derived fingerprint values for a plurality of unique programs to be broadcast are stored (Col. 4, lines 52-67; Col. 5, lines 1-26; Col. 7, lines 4-29);

registering said unique watermark and associated derived fingerprint value for said program to be broadcast in said database (Col. 4, lines 52-67; Col. 5, lines 1-26; Col. 7, lines 4-29); and

redundantly identifying said broadcast program, e.g. a watermark containing additional information for use in conjunction with a content signature, i.e. fingerprint (Col. 6, lines 40-52; Col. 6, line 65-Col. 7, line 50; Col. 8, line 64-Col. 9, line 4). The content signature can be used to determine a content ID, licensing or registration data, other metadata, etc (Col. 1, lines 50-64; Col. 5, lines 15-26; Col. 6, line 65-Col. 7, line 3). The watermark can be used to determine owner ID, metadata, security information, copy control data, etc (Col. 6, line 65-Col. 7, line 3);

said redundant identification comprising:

comparing any detected watermark value with said database of registered watermark values (Col. 7, lines 4-29);

if a detected watermark value matches a registered watermark value from said database of registered watermark values, cross-checking said fingerprint value derived from said given broadcast program against said database of registered fingerprints (Col. 3, lines 20-40; Col. 4, lines 52-67; Col. 5, lines 1-26; Col. 6, lines 14-32; Col. 7, lines 4-30); and

if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint to assess a status of said broadcast program, i.e. the fingerprint and watermark are compared and determines the content to be authentic or modified (Col. 6, lines 39-52), Note: the fingerprint and the watermark may both contain the same information and when compared the information will coincide and prove the content to be authentic or will be different and prove the content to be modified in some way.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar to redundantly identify said broadcast program, said redundant identification comprising: if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint to assess a status of said broadcast program, using the known watermarking and fingerprinting technique as well as the known content-identifying technique taught by Brunk in combination with the watermarking and fingerprinting technique of Alattar, for the purpose of providing an extra layer of security for media content and to provide a content verification tool.

Regarding claim 4, Alattar in view of Brunk teaches said program to be broadcast has an associated embedded audio data stream (Alattar-Col. 2, lines 7-10 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar); and

said unique watermark is encoded into the bits of said program's embedded audio data stream, i.e. tag in a file header (Alattar-Col. 3, lines 55-57 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar).

Regarding claim 6, Alattar in view of Brunk teaches reporting the results of said cross-checking to a registrant of said program to be broadcast, i.e. data is determined to be authentic or modified; user is presented with all matches (Brunk-Col. 6, lines 39-52; Col. 9, lines 33-37; Col. 12, lines 34-48).

Regarding claim 7, Alattar in view of Brunk teaches comparing said fingerprint value derived from said given broadcast program with all said stored fingerprint values when said fingerprint value derived from said given broadcast program is different than said stored fingerprint value associated with said stored watermark, i.e. recalculated content signature is compared to stored signatures in a database (Brunk-Col. 12, lines 34-48).

Regarding claim 10, Alattar teaches a method for enabling reliable identification of a content comprising:

embedding a watermark value into said content to produce an embedded content (Col. 5, lines 56-63);

generating a fingerprint associated with said content (Col. 20, lines 9-17);

registering information comprising said watermark value, wherein said information can be subsequently used to identify said content, i.e. the watermark may contain broadcast monitoring, creator, distributor, and recipient information as well as identifying which movie was broadcast, who broadcast it, and when it was broadcast (Col. 8, lines 13-36, Col. 8, line 61-Col. 9, line 4; Col. 10, lines 10-18; Col. 4, lines 1-19 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar), said identification comprising:

generating a fingerprint associated with a received content (Col. 20, lines 15-17);

analyzing said received content to detect at least one watermark value (Col. 1, lines 29-39; Col. 3, lines 10-17; Col. 8, lines 24-28; Col. 20, lines 46-51);

identifying said received content by comparing said detected watermark value with a database of registered watermark values, Note: a watermark value, according to Alattar, not only serves as a calibration signal but also can include identifiers, that relate the identifiers from the watermark to corresponding

identifiers in a database that has additional information to identify the content owner, distributor, etc (Col. 10, lines 10-18);

if said detected watermark value matches a registered watermark value from said database of registered watermark values, said fingerprint is compared with a database of registered fingerprints (Col. 20, lines 38-57).

Alattar does not clearly teach registering information comprising said watermark value and said fingerprint, wherein said information can be subsequently used to redundantly identify said content, said redundant identification comprising: if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content.

Brunk, explicitly incorporated by reference in Alattar (Col 20, Lines 26-35) teaches embedding a content signature in a watermark and registering a content signature in a database; the watermark and content signature are used to redundantly identify a content item (Col. 2, lines 40-65; Col. 6, line 65-Col. 7, line 3), said redundant identification comprising:

identifying said received content by comparing said detected watermark value with a database of registered watermark values (Col. 7, lines 4-29);

if a detected watermark value matches a registered watermark value from said database of registered watermark values, said fingerprint is compared with a database of registered fingerprints (Col. 3, lines 20-40; Col. 4, lines 52-67; Col. 5, lines 1-26; Col. 6, lines 14-32; Col. 7, lines 4-30); and

if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint to assess a status of said broadcast program, i.e. the fingerprint and watermark are compared and determines the content to be authentic or modified (Col. 6, lines 39-52), Note: the fingerprint and the watermark may both contain the same information and when compared the information will coincide and prove the content to be authentic or will be different and prove the content to be modified in some way.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar to include registering information comprising said watermark value and said fingerprint, wherein said information can be subsequently used to redundantly identify said content, said redundant identification comprising: if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content, using the known watermarking and

fingerprinting technique as well as the known content-identifying technique taught by Brunk in combination with the watermarking and fingerprinting technique of Alattar, for the purpose of providing an extra layer of security to a media content and to provide a content verification tool.

Regarding claim 11, Alattar in view of Brunk teaches said fingerprint is generated by analyzing inherent characteristics of the content (Alattar-Col. 20, lines 9-17).

Regarding claim 12, Alattar in view of Brunk teaches said inherent characteristics comprise at least one of luminance, chroma, gamma, or amplitude levels of the content (Alattar-Col. 20, lines 9-17).

Regarding claim 13, Alattar in view of Brunk teaches said fingerprint is generated for at least portions of an audio or video component of said signal (Alattar-Col. 20, lines 9-17).

Regarding claim 14, Alattar in view of Brunk teaches said watermark value is embedded in at least portions of an audio or video component of said content (Alattar-Col. 5, lines 56-63).

Regarding claim 17, Alattar in view of Brunk teaches receiving information comprising at least said watermark value and said fingerprint at a registration authority (Alattar-Col. 10, lines 10-18; Col. 4, lines 1-19 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar; Brunk-Col. 2, lines 40-65); and

verifying the received information, i.e. verifying that the content is authentic or modified (Brunk-Col. 2, lines 40-65, Col. 6, lines 40-53; Alattar-Col. 10, lines 10-18; Col. 20, lines 49-55).

Regarding claim 18, Alattar in view of Brunk teaches comparing at least one of said watermark value or said fingerprint against a database of registered watermark values and fingerprints (Alattar-Col. 10, lines 10-18; Col. 20, lines 49-55; Brunk-Col. 7, lines 4-30).

Regarding claim 19, Alattar in view of Brunk teaches registering is completed when said comparing produces no matches (Col. 10, lines 29-36 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar).

Regarding claim 24, Alattar in view of Brunk teaches receiving additional content identification information (Alattar-Col. 5, lines 59-63; Col. 3, line 65-Col.

4, line 14 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar).

Regarding claim 25, Alattar in view of Brunk teaches said additional content identification information comprises at least one of content title, ownership information, or origination information (Col. 5, lines 59-63; Col. 3, line 65-Col. 4, line 14 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar).

Regarding claim 26, claim is analyzed with respect to claim 18.

Regarding claim 27, claim is analyzed with respect to claim 19.

Regarding claim 32, Alattar teaches a method for enabling identification of a received content comprising: generating a fingerprint associated with said received content (Col. 20, lines 15-17);

analyzing said received content to discern the presence of embedded watermarks (Col. 1, lines 29-39; Col. 3, lines 10-17; Col. 8, lines 24-28; Col. 20, lines 46-51); and

identifying said received content in accordance with a plurality of registered fingerprint and watermark values, i.e. the watermark may contain broadcast monitoring, creator, distributor, and recipient information as well as identifying which movie was broadcast, who broadcast it, and when it was broadcast (Col. 10, lines 10-36; Col. 20, lines 39-57; Col. 4, lines 1-19 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar), wherein:

at least one watermark value is detected as a result of said analyzing (Col. 1, lines 29-39; Col. 3, lines 10-17; Col. 8, lines 24-28; Col. 20, lines 46-51);

said identifying comprises comparing a detected watermark value with a database of registered watermark values (Col. 20, lines 50-55);

matching a content signature with a registered content signature (Alattar-Col. 20, lines 38-59).

Alattar does not clearly teach identifying said received content by redundant utilization of both of said generated fingerprint and said analyzing; if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content.

Brunk, explicitly incorporated by reference in Alattar (Col 20, Lines 26-35) teaches a watermark containing additional information for use in conjunction with

a content signature, i.e. fingerprint (Col. 6, lines 40-52; Col. 6, line 65-Col. 7, line 50). The content signature can be used to determine a content ID, licensing or registration data, other metadata, etc (Brunk-Col. 1, lines 50-64). The watermark can be used to determine owner ID, metadata, security information, copy control data, etc (Brunk-Col. 6, line 65-Col. 7, line 3); and

a watermark containing a content signature is matched to a corresponding watermark value, then once matched, forwarding the content signature to the owner's database where it is matched to song information (Col. 3, lines 20-40; Col. 4, lines 52-67; Col. 5, lines 1-26; Col. 6, lines 14-32; Col. 7, lines 4-30);

said identifying comprises comparing the detected watermark value with a database of registered watermark values (Col. 34, lines 34-47);

if the detected watermark value matches a registered watermark value from the database, said fingerprint is compared with a database of registered fingerprints, i.e. a watermark is sent to a database and is matched to a registered watermark which contains owner information then forwarding the content signature to the owner's database where it is matched to the registered content signature and song information (Brunk-Col. 7, lines 4-30); and

matching a content signature with a registered content signature (Col. 1, lines 50-65; Col. 5, lines 1-26; Col. 6, lines 14-33);

comparing a watermark with a content signature to determine if the content is authentic or modified (Col. 6, lines 39-53; Col. 7, lines 4-30), Note: the

watermark and the content signature have to have identification information present in order to determine whether or not they match.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar to include to include identifying said received content by redundant utilization of both of said generated fingerprint and said analyzing; if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content, using the known watermarking and fingerprinting technique as well as the known content-identifying technique taught by Brunk in combination with the watermarking and fingerprinting technique of Alattar, for the purpose of providing an extra layer of security to a media content and to provide a content verification tool.

Regarding claim 33, Alattar in view of Brunk teaches identifying is based on additional information stored in a registration database, i.e. version number stored in a system (Alattar-Col. 9, lines 14-21).

Regarding claim 36, Alattar in view of Brunk teaches at least one watermark is detected as a result of said analyzing (Alattar-Col. 1, lines 29-39;

Col. 3, lines 10-17; Col. 8, lines 24-28; Col. 20, lines 46-51; Brunk-Col. 2, lines 10-33); and

the detected watermark and said fingerprint are combined to uniquely identify said received content (Alattar-Col. 20, lines 25-29; Brunk- Col. 2, lines 10-33; Col. 6, line 65-Col. 7, line 3).

Regarding claim 38, Alattar in view of Brunk teaches an agreement between said first and second identification information indicates the reception of a properly registered content, i.e. content is authentic (Brunk-Col. 6, lines 39-53; Col. 7, lines 4-30).

Regarding claim 40, Alattar in view of Brunk teaches a conflict between said first and second identification information indicates the reception of an improperly registered content or an altered content, i.e. content is modified (Brunk-Col. 6, lines 39-53; Col. 7, lines 4-30).

Regarding claim 42, Alattar in view of Brunk teaches cryptographic techniques are employed to ensure secure communications with said database, i.e. using private keys for accessing a private database (Alattar-Col. 12, lines 49-63; Brunk-Col. 7, lines 29-50).

4. Claims 3, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alattar in view of Brunk and further in view of Baker (6,912,010).

Regarding claim 3, Alattar in view of Brunk teaches all elements of claim 2.

Alattar in view of Brunk does not teach said unique watermark value is written into the user bits of said program's SMPTE time code.

Baker teaches a source ID is written into the user bits of the program's SMPTE time code (Col. 1, lines 44-48; Col. 2, lines 20-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk's watermark embedding technique to include writing the watermark value into the user bits of a vertical interval time code for the purpose of saving program signal bandwidth.

Regarding claim 15, Alattar in view of Brunk teaches all elements of claim 10.

Alattar in view of Brunk does not teach a source ID is inserted into an auxiliary information area of said content.

Baker teaches said watermark value is inserted into an auxiliary information area of said content (Col. 1, lines 44-48; Col. 2, lines 20-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk's watermark

embedding technique to include writing the watermark value into the user bits of a vertical interval time code for the purpose of saving program signal bandwidth.

Regarding claim 16, Alattar in view of Brunk and further in view of Baker (Col. 1, lines 44-48) teaches said auxiliary information area is reserved for an SMPTE time code.

5. Claims 20-23 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alattar in view of Brunk and further in view of Nicholas (US 2002/0054089).

Regarding claim 20, Alattar in view of Brunk teaches all elements of claims 10, 17, and 18.

Alattar in view of Brunk does not clearly teach production of at least one match as a result of said comparing is indicative of an incomplete registration.

Nicholas teaches a website registration process in which a user registers for a website by providing a username and password. If the username is already being used by another customer, then the registration is incomplete and the user is notified to enter a different username (Para. 43).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk's registration process to use the known registration process taught by Nicholas. Known work in one field of endeavor, i.e. website registration, may prompt variations of it for

use in either the same field or a different one, i.e. watermark/fingerprint registration, based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

Regarding claim 21, Alattar in view of Brunk in view of Nicholas teaches notifying at least one of an applicant or a content owner, i.e. if the username is already being used by another customer, then the user is notified to enter a different username (Nicholas-Para. 43).

Regarding claim 22, Alattar in view of Brunk teaches all elements of claims 10, 17, and 18.

Alattar in view of Brunk does not clearly teach registering is partially completed when said comparing produces at least one match.

Nicholas teaches a website registration process in which a user registers for a website by providing a username and password. If the username is already being used by another customer, then the registration is incomplete and the user is notified to enter a different username (Para. 43).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk's registration process to use the known registration process taught by Nicholas. Known work in one field of endeavor, i.e. website registration, may prompt variations of it for

use in either the same field or a different one, i.e. watermark/fingerprint registration, based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

Regarding claim 23, Alattar in view of Brunk in view of Nicholas teaches contacting at least one of an applicant for registration or a content owner, i.e. if the username is already being used by another customer, then the user is notified to enter a different username (Nicholas-Para. 43); and

updating said database in accordance with the response(s) of said applicant or said content owner, i.e. the user enters a unique username and the database is updated with the new username (Nicholas-Para. 43; Alattar-Col. 10, lines 24-30; Col. 10, lines 29-36 of US 6,505,160 which is incorporated by reference from Col. 10, lines 30-36 of Alattar).

Regarding claim 28, claim is analyzed with respect to claim 20.

Regarding claim 29, claim is analyzed with respect to claim 21.

Regarding claim 30, claim is analyzed with respect to claim 22.

Regarding claim 31, claim is analyzed with respect to claim 23.

6. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alattar in view of Brunk in view of Serret-Avila (US 6,785,815) and further in view of Nakamura (US 6,915,422).

Regarding claim 35, Alattar in view of Brunk teaches all elements of claim 32.

Alattar in view of Brunk further teaches said identifying comprises comparing said fingerprint with a database of registered fingerprints (Alattar-Col. 20, lines 50-55; Brunk-Col. 12, lines 34-47).

Alattar in view of Brunk does not clearly teach no watermarks are detected as a result of said analyzing; and if no fingerprint matches are discovered, reporting the reception of an unregistered content.

Serret-Avila teaches content, when registered, includes a strong watermark and a digital signature included in a weak watermark (Col. 6, lines 60-67). When a user attempts to access media, it is checked for the presence of the strong watermark and the digital signature. (Col. 6, lines 32-45; Col. 6, line 66-Col. 7, line 21). If no watermark is found, the content is determined to be unregistered (Col. 6, line 66-Col. 7, line 21).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk to include if no

watermarks are detected as a result of said analyzing; and if no fingerprint matches are discovered, determining the reception of an unregistered content, as taught by Serret-Avila, for the purpose of inhibiting the use of previously-registered content that has been improperly modified (Serret-Avila-Col. 7, lines 17-21).

Alattar in view of Brunk in view of Serret-Avila does not clearly teach reporting the reception of an unregistered content.

Nakamura teaches a process wherein a host checks whether or not a user is registered by determining if the user's telephone number is stored in a database. If not, the user is determined to be unregistered and an unregistered notification screen is displayed to the user (Col. 8, line 55-Col. 9, line 8).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk to include reporting the reception of an unregistered content, using the known process of displaying an unregistered notification screen taught by Nakamura. Known work in one field of endeavor, i.e. user registration, may prompt variations of it for use in either the same field or a different one, i.e. watermark/fingerprint registration, based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

7. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alattar in view of Brunk and further in view of Zhao (US 6,487,301).

Regarding claim 39, Alattar in view of Brunk teaches all elements of claim 32.

Alattar in view of Brunk teaches in the event of a conflict between said first and second identification information the content is considered to be modified (Brunk-Col. 6, lines 39-53; Col. 7, lines 4-30).

Alattar in view of Brunk does not clearly teach issuing a report.

Zhao teaches sending an indication of whether content is authentic or modified to the source of the content (Col. 16, lines 36-55; Col. 17, lines 22-57; Col. 18, lines 1-6).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Alattar in view of Brunk to include issuing a report in the event of a conflict between an identification information in a watermark and identification information in a fingerprint, as taught by Zhao, so as to enable an owner to pursue a copyright infringement violator (Zhao-Col. 3, lines 4-30).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMY DUFFIELD whose telephone number is (571)270-1643. The examiner can normally be reached on Mon.-Thurs. 8:00 A.M.-5:30 P.M. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Beliveau can be reached on (571) 272-7343. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

27 August 2009
JSD

/Scott Beliveau/
Supervisory Patent Examiner, Art Unit 2427